REMARKS/ARGUMENTS

The Office Action has been carefully considered. Claims 1-6, 8-19, 34-36, 38-39, 41-43, 45-52, 54, and 56-61 are pending. In the Office Action, pending claims were rejected in the following manner.

1. Claims 49-52, 54, and 56-61 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.
2. Claims 1-2, 12, 34-35, 49, and 50 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.
3. Claims 1-4, 8-9, 11-19, 31, 34-36, 38-39, 41-42, 45-52, 54, 56-57, and 59-61 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Nonaka et al's US Publication No. 2003/0046238 (hereinafter "*Nonaka*") in view of Hall et al's US Patent No. 7,062,500 (hereinafter "*Hall*") and further in view of Hardy et al's US Patent No. 6,079,018 (hereinafter "*Hardy*") and Thoma et al's US Publication No. 2002/0152393 (hereinafter "*Thoma*").
4. Claims 5-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma*, and further in view of Serret-Avila et al's US Patent No. 6,959,384 (hereinafter "*Serret-Avila*").
5. Claims 10, 32-33, 43 and 58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma* and further in view of Chase Jr. et al's US Patent No. 7,080,043 (hereinafter "*Chase*").

At the onset, Applicant respectfully notes the following concerns regarding the previous Office Action. Namely, upon Applicant review of the stated reasons in the Office Action for rejection of Claims 5-6 and 32-33 it appears that the Office may not have been examining the most recent version of the amended claims. Applicant respectfully suggests that the Office, upon full consideration of Applicant's amendments and remarks, issue either a notice of allowance or another **non-final Office Action** so as to provide the Applicants fair opportunity to reply to any rejections. The reasons for asserting that the most recent version of the amended claims may not have been examined are clarified below.

Claims 32 and 33

Claims 32 and 33 were rejected along with Claims 10, 43, and 58 in item 11 on page 31 of the Office Action under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma* and further in view of *Chase*. Upon review of the stated reasons for rejection of Claims 32 and 33 it appears that the Office Action may not have been examining the most recent version of the amended claims. Accordingly, Applicant respectfully traverses.

More specifically, Applicant notes that the Office Action specifically references Claim 32 and Claim 33, both of which were previously canceled, in the rejection on page 31. While the inclusion of these canceled claims may simply be disregarded as moot, Applicant is concerned that the Office Action may not have been examining the most recent version of the amended claims and as a result "all words in a claim" were not by definition considered in judging the patentability of Claims 10, 43, and 58 as required under MPEP § 2143.03. When this concern is combined with the fact that supporting any rejection under 35 U.S.C. § 103(a) requires a clear articulation of the reasons why the claimed invention would have been obvious (MPEP § 2143), sufficient grounds exist to request specific clarification **in a non-final Office Action.** Accordingly, Applicants respectfully request further clarification of the rejection of Claims 10, 43, and 58 under 35 U.S.C. § 103(a) **in a non-final Office Action** so as to provide the Applicants fair opportunity to reply to the rejection.

Claims 5-6

Claims 5-6 were rejected under 35 U.S.C. § 103(a) in item 10 on page 29 of the Office Action as being unpatentable over a proposed combination of *Nonaka-Hall-Hardy-Thoma*, and further in view of *Serret-Avila*. Upon review of the stated reasons for rejection of Claims 5-6 it appears that the Office Action may not have been examining the most recent version of the amended claims. Accordingly, Applicant respectfully traverses.

As previously stated, the key to supporting any rejection under 35 U.S.C. § 103(a) is the clear articulation of the reasons why the claimed invention would have been obvious. (MPEP § 2143). Unfortunately, as indicated below, this was not the case with the claim rejections of Claim 5 and Claim 6 as presented in the Office Action.

Claim 5 calls for, *inter alia*, the method of claim 1 further including "receiving the external key at the client device."

Claim 6 calls for, *inter alia*, the method of claim 2 such that "said external key comprises a server device key."

Despite MPEP § 2143.03 requiring that "All words in a claim must be considered in judging the patentability of that claim against the prior art" it appears that neither of the claim limitations in Claim 5 or Claim 6 are directly addressed by the Office Action. Rather it appears the Office Action is referring to the original claims or at least claims prior to the Amendment submitted on April 22, 2008.

More specifically, in reference to Claim 5, the Office Action refers to "the capability to generate a second integrity hash using a first integrity hash" on page 30 and "storing the integrity hash in a clear form" on page 29. Both are limitations no longer present in Claim 5. While many of the original limitations in Claim 5 were incorporated into independent Claim 1, the Office Action does not specifically address the existing limitations of Claim 5, namely that "the external key" is received "at the client device."

Similarly, the section of the Office Action dedicated to Claim 6 on page 30 indicates "*Nonaka* discloses the method of claim 5" and further references "receiving the second integrity hash from a server". Clearly, Claim 6 is not dependent on Claim 5. Moreover, there is no mention of the second integrity hash in Claim 6, but rather the external key limitation is further clarified to be a server device key in Claim 6.

Applicant respectfully notes that it is important for an Office Action to properly communicate the basis for a rejection so that the issues can be identified early and the Applicant can be given fair opportunity to reply (see e.g., MPEP 706.02(j) and 707.07(d) which indicate that "the ground of rejection [be] fully and clearly stated"). Moreover, as the rejection is based on the proposed combination of *Nonaka,Hall, Hardy,* and *Thoma* it is also believed that Claim 5 and Claim 6 would also be allowable for at least the same reasons outlined below for Claim 1. Accordingly, Applicant respectfully requests withdrawal of the rejections under 35 U.S.C. § 103(a) to Claim 5 and Claim 6.

Alternatively, Applicants respectfully request further clarification of the rejection of Claim 5 and Claim 6 under 35 U.S.C. § 103(a) **in a non-final Office Action** so as to provide the Applicants fair opportunity to reply to the rejection.

35 U.S.C. § 101 Rejections

Claims 49-52, 54, and 56-61 were objected to as being directed to non-statutory subject matter. More specifically, the Office Action indicates in item 5 on page 5 that the rejected claims appear to cover both "transitory" and "non-transitory" machine-readable medium. The Office's suggested corrections to Claims 49-52, 54, and 56-61 have been made to include the "non-transitory" limitation in accordance with the aforementioned Office Action. Accordingly, withdrawal of this objection is respectfully requested.

35 U.S.C. § 112 Rejections

Claims 1, 2, 12, 34, 35, 49, and 50 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

More specifically, the Office Action alleges that there does not appear to be disclosure for the claim limitations "wherein said integrity secret is vulnerable based at least in part on its being known" and "said internal integrity hash is not vulnerable based on said vulnerability of said externally-known integrity secret" associated with Claims 1, 34, and 49. The Examiner further indicates interpretation of these claim limitations to include that a secret is known by an external system and that the secret is protected utilizing some mechanism.

Applicant has amended Claims 1, 34, and 49 to clarify that "said internal integrity hash is not vulnerable based on **a relative comparison with** said vulnerability of said externally known integrity secret" and respectfully traverse this rejection. Support for the amendments to Claims 1, 34, and 49 may be found, among other places, in the specification of the instant application (*e.g.*, paragraph [0022]), which states:

> [0022] In order to use hash 120 to test the integrity of license 110, external secret 122 **is known external to the client device**. Any of a variety of approaches can be used to try to maintain the security of secret 122, but, unfortunately, **any secret known outside the client device is likely to be vulnerable**. A sophisticated and determined user is likely to gain access to secret 122 eventually. But, **even if hash 120 is compromised, the illustrated embodiment includes a second layer of security and integrity that does**

> **not rely on an externally known secret**, namely internal security block 130. (emphasis added)

Accordingly, as indicated in paragraph [0022], the "integrity secret" of Claims 1, 34, and 49 is known external to the client device and "any secret known outside the client device is likely to be vulnerable" to a sophisticated and determined user. Since the "internal integrity hash" is not known outside of the client device, it is not subject to the same vulnerability, relative to the sophisticated and determined user, that is present in the "integrity secret" of Claims 1, 34, and 49. Additional support may be found in the original claims of the instant application (*e.g.*, Claims 19 and 20) and the original figures of the instant application (*e.g.*, FIG 11A and 11B). It is believed that no new matter has been introduced as a result of this amendment. Accordingly, withdrawal of this objection is respectfully requested.

The Office Action further alleges that there is no disclosure within the specification or original claims of the term "external server" as used in Claims 2, 12, 35, and 50. Applicant respectfully notes that the full term is "external server device" as seen in Claims 2, 12, 35, and 50 not just "external server" as indicated in the rejection described in item 7 on page 6 of the Office Action. While the exact term "external server" is not used previously, both "server device" and "external device" are explicitly mentioned in at least one of paragraphs [0005], [0006], [0017], [0021], and [0035] of the specification. Moreover in at least one instance, the specific example given of the "external device" is a "server device" making use of an external server device a reasonable description as demonstrated in the excerpt from [0005] of the specification below:

> In which case, **the client device** usually needs an application program interface (API) to manage communications with **an external device**. For example, if **a client device** stores the rights and/or usage information in encrypted form, **a server device** may need to establish communications with **the client device** through an API.
>
> (*emphasis added*, [0005] of the specification)

As an external server is clearly a subset of the external device or at the very least an extension of the server device described within the specification, Applicant respectfully asserts that sufficient disclosure exists to reasonably convey to one skilled in the relevant art

that the inventor had possession of the claimed invention. Accordingly, withdrawal of this objection is also respectfully requested.

35 U.S.C. § 103(a) Rejections

Claims 1-4, 8-9, 11-19, 31, 34-36, 38-39, 41-42, 45-52, 54, 56-57, and 59-61

Claims 1-4, 8-9, 11-19, 31, 34-36, 38-39, 41-42, 45-52, 54, 56-57, and 59-61 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka* in view of *Hall* and further in view of *Hardy* and *Thoma*. Applicant respectfully traverses.

To establish a *prima facie* case of obviousness, an Office Action must demonstrate that all claimed elements are taught or suggested by proffered prior art references. In fact, "consideration" of every claim feature is required in an obviousness determination. More specifically, MPEP § 2143.03 indicates that "All words in a claim must be considered in judging the patentability of that claim against the prior art".

To render a claim unpatentable, however, the Office must do more than merely "consider" each and every feature for this claim. Instead, the asserted combination of cited references must also teach or suggest *each and every claim feature*. *See In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) (emphasis added) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art).

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103, despite any recent revision to the MPEP. For example, in *In re Wada and Murphy,* Appeal 2007-3733, the BPAI specifically states that:

> "When determining whether a claim is obvious, an examiner must make "a searching comparison of the claimed invention – *including all its limitations* – with the teaching of the prior art." *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis added). Thus, "obviousness requires a suggestion of all limitations in a claim." *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) (*citing In re Royka*, 490 F.2d 981, 985 (CCPA 1974)). Moreover, as the Supreme Court recently stated, "*there must be some articulated reasoning* with some rational underpinning to support the

legal conclusion of obviousness." *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007) (quoting In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006) (emphasis added))."

In sum, it remains well-settled law that obviousness requires **at least a suggestion of all of the elements of a claim**. *See In re Wada and Murphy, citing CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) and *In re Royka*, 490 F.2d 981, 985 (CCPA 1974)). Moreover, it is "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements **in the way the claimed new invention does**." *KSR*, 127 S.Ct. at 1741.

As amended Claim 1 now reads, *inter alia*, the method comprising:

obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client device;

obtaining, by said client device, **an external key comprising an integrity secret**, wherein said integrity secret is **vulnerable** based at least in part on its **being known to at least an external server device**;

obtaining **a clear form external integrity hash** of first data comprising:

said clear form rights information and

said external key,

wherein said clear form **external integrity hash is vulnerable** based at least in part **on said vulnerability of said externally-known integrity secret**;

obtaining **an internal integrity hash** of second data comprising

said clear form rights information,

said clear form external integrity hash, and

an **externally inaccessible client device key**,

wherein said externally inaccessible client device key is **not accessible outside said client device** and **said internal integrity hash is not vulnerable based on a relative comparison with said vulnerability of said externally-known integrity secret**;

encrypting said internal integrity hash using said externally inaccessible client device key; and

storing **the encrypted internal integrity hash on the client device**.

Similar claim language is also found in Claims 34 and 49.

As previously clarified, Applicant amended Claims 1, 34, and 49 to clarify that "said internal integrity hash is not vulnerable based on **a relative comparison with** said vulnerability of said externally known integrity secret." The "integrity secret" of Claims 1, 34, and 49 is known external to the client device and as such is likely to be vulnerable to a sophisticated and determined user. Since the "internal integrity hash" is not known outside of the client device, it is not subject to the same vulnerability. This relative security enables a client device using the present invention to store rights information in clear form to reduce overall processing, while still maintaining an internal integrity hash that is comparatively secure relative to the vulnerability of the externally-known integrity secret.

In comparison, *Nonaka* discloses data processing for suitably protecting the profits of a content-rights holder, such as a content provider. (*see e.g.*, paragraph [0017] of *Nonaka*). In essence, *Nonaka* discloses a method of distributing encrypted content data from an electronic music distribution center to users. More specifically, *Nonaka* describes rights processing of content data, encrypted with content key data, based on usage control policy data including decrypting the encrypted content key data that is placed within a tamper-resistant circuit module. (*see e.g.*, paragraph [0019], [0245]-[0246] of *Nonaka*). This tamper-resistant circuit module is also referred to as a secure application module (SAM) ([0069] of *Nonaka*) and is illustrated as one of the modules within the key file data structure shown in Fig. 5 of *Nonaka*. A SAM of *Nonaka* may be delivered from the content provider to the client device and often incorporates key security mechanisms, such as public and private key, that may be synchronized or authorized by content provider (e.g., content provider 101) or by a root certifying authority 92. However, all of the key mechanisms of *Nonaka*, such as the content key and signature key, employ security measures, externally known to the client device, and as such may be discovered by a sophisticated and determined user. Moreover, the mechanisms employed by *Nonaka* require far more processing than the instant invention that maintains portions of data in clear form rather than encrypting the entire contents of the data module.

Accordingly, *Nonaka* specifically does not include storing rights information in a "clear" form (Page 8 of Office Action) as recited in claim 1 of the instant application. Furthermore, *Nonaka* does not teach the combination of "an internal integrity hash" that

includes "clear form rights information", "clear form external integrity hash", and "an externally inaccessible client device key" as recited in claim 1 of the instant application.

In further contrast to the instant application, *Hall* discloses descriptive data processing including defining, using, and manipulating rights management data structures. The rights management data structure may include integrity constraints that state rules about associated information. (Abstract of *Hall*). Accordingly, the rights management data structure are maintained as a "container moves from one entity to another." The descriptive data structure (DDS) provides an electronically enforced chain of handling and control. This may allow content rights holders to securely control and manage content, events, transaction, rules, and usage consequences, including any required payment or usage reporting. (col. 2, lines 4-14 of *Hall*). *Hall* also describes maintaining machine readable descriptive data structures (DDS) in a "clear" form so they are easily accessible. (col. 6, lines 19-22 of *Hall*). Moreover, *Hall* indicates that DDS may themselves be packaged within rights management data structures, and that additional rules controlling their access and use may be associated with the outer data structure.

However, the proposed combination of *Nonaka-Hall* does not include disclosure of a hash comprising a hash and an encryption key. (Page 8 of the Office Action). Moreover, *Nonaka-Hall* does not teach "an internal integrity hash" that includes "clear form rights information", "clear form external integrity hash", and "an externally inaccessible client device key" as recited in claim 1 of the instant application.

Comparatively, *Hardy* discloses generating unique secure values for digitally signing documents. A document is signed using a unique digital signature. A document digest is generated by applying a hash function to the digitally signed document. A pseudo-random key is created by combining the resulting document digest with a predefined computation procedure. This predefined computation procedure may include combining the document digest with a private key and hashing the resulting value. (Abstract of *Hardy*). Alternatively, Hardy also describes generating the pseudo-random key by hashing a private key and then combining the result of the hash with an ancillary secret value and the document digest and hashing this second result. (Abstract of *Hardy*).

However, the proposed combination of Nonaka-*Hall-Hardy* does not include a device key being externally inaccessible from the client device and a vulnerability mechanism.

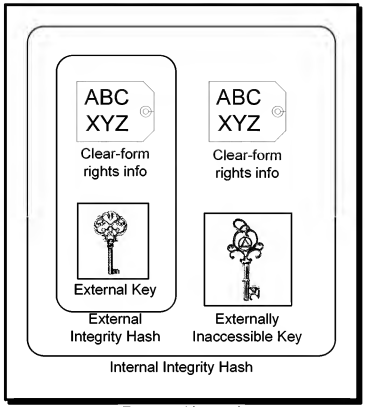
(Page 8 of Office Action). Additionally, *Hardy* also fails to teach or suggest a second internal integrity hash generated from (1) rights information; (2) an externally inaccessible key; and (3) a first external integrity hash that itself comprise (a) **the same rights information as in the second hash**, and (b) an external key. More specifically, *Nonaka-Hall-Hardy* does not teach "an internal integrity hash" that includes "clear form rights information", "clear form external integrity hash", and "an externally inaccessible client device key" as recited in claim 1 of the instant application.

In further comparison, *Thoma* discloses a secure extensible computing environment. More specifically, *Thoma* teaches downloading encrypted e-content to a terminal device. (Abstract of *Thoma*). *Thoma* teaches use of a symmetric key to encrypt content and use of both a private and public key to encrypt the symmetric key. More specifically, the content server uses a public key of a public-private key pair associated with a terminal device to encrypt the symmetric key and the terminal device then uses a private key of the public-private key pair associated with the terminal device to obtain the symmetric key. ([0035] of *Thoma*). Use of public-private key pair encryption in *Thoma* is distinguishable from hash algorithms on both a computational and cryptographic level.

Clearly, the proposed combination of *Nonaka-Hall-Hardy- Thoma* does not teach "an internal integrity hash" that includes "clear form rights information", "clear form external integrity hash", and "an externally inaccessible client device key" as recited in claim 1 of the instant application.

In contrast to the proposed combination of *Nonaka-Hall-Hardy-Thoma*, Claim 1 of the instant application is directed to an encrypted "internal integrity hash", which comprises "clear form rights information", a hash comprising the same clear-form rights information (e.g., "said clear form external integrity hash"), and which further comprises "an externally inaccessible client device key" that is not accessible outside said client device. In other words, there is an externally inaccessible key combined with the clear form information and a hash of a hash of the clear-form rights information, which also includes the same clear-form rights information (e.g., "said clear form rights information"). This is a concept that is simply not taught or suggested by *Nonaka*, *Hall*, *Hardy* or *Thoma*, either alone or in any combination thereof.

A visual depiction of this unique "internal integrity hash" described in Claim 1 is provided below.



Encrypted Internal Integrity Hash of Claim 1

As shown above, the encrypted internal integrity hash comprises two copies of the clear form rights information. Specifically, a first copy of the clear form rights information is in the external integrity hash, and a second copy of the clear form rights information is in the internal integrity hash (which also includes the external integrity hash).

It is accordingly believed to be clear that the proposed combination of *Nonaka*, *Hall*, *Hardy* and *Thoma* neither shows nor suggests the features of Claim 1. Similar language is used in independent Claim 34 and independent Claim 49. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103(a) to the Claims 1, 34, and 49 is respectfully requested.

Dependent Claims 2-6,8-9,11-19,31, 35-36,38-39,41-42,45-48,50-52,54,56-57, and 59-61

MPEP §2143.03 clarifies that if an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is also nonobvious. (In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)). Accordingly, the dependent Claims 2-6, 8-9,

11-19, and 31 are believed to be patentable as well because they all are ultimately dependent on Claim 1, which was previously shown to be nonobvious. Dependent Claims 35-36, 38-39, 41-42, and 45-48 are also believed to be patentable as well because they all are ultimately dependent on nonobvious Claim 34. Dependent Claims 50-52, 54, 56-57, and 59-61 are also believed to be patentable as well because they all are ultimately dependent on nonobvious Claim 49. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103(a) to Claims 2-6, 8-9, 11-19, 31, 35-36, 38-39, 41-42, 45-48, 50-52, 54, 56-57, and 59-61 is also respectfully requested.

While the dependent Claims 2-6, 8-9, 11-19, 31, 35-36, 38-39, 41-42, 45-48, 50-52, 54, 56-57, and 59-61 are believed to be patentable due to their dependence on the independent claims, each dependent claim also introduces at least one new element that Applicants believe make the dependent claims individually patentable.

Clear Form Element of Claims 1-2,4,9,11-13,17-18,34-35,38,42,45,47,49-50,52,57,and 59-61

Use of clear form rights information within a secure hash is distinctive over cited references. In particular, of the cited references in the Office Action only *Hall* indicates the use of data maintained in a "clear" form. However, while *Hall* does disclose the potential use of "clear" form data, *Hall* also **expressly** limits application of "clear" form data to "machine readable descriptive data structures" free from encryption. Specifically, *Hall* clarifies that "Some machine readable descriptive data structures may be encrypted in whole or part, while others might be maintained in 'clear' form so they are easily accessible." (col. 6, lines 19-22 of *Hall*). This statement in *Hall* intentionally creates two mutually exclusive groups, a first encrypted group (in whole or in part) and a second clear group. As previously described, the instant application expressly utilizes clear form rights information within a secure hash thereby meshing encryption and clear form rights information. In fact, some embodiments include multiple copies of the clear form rights information each coupled with an encryption key (e.g., externally inaccessible key and/or external key) that are embedded into a hash layer. More specifically, Claims 1, 2, 4, 9, 11-13, 17, 18, 34, 35, 38, 42, 45, 47, 49, 50, 52, 57, and 59-61 each include an internal integrity hash with "clear form rights information" and all were rejected under 35 U.S.C. § 103(a) as being unpatentable over proposed combinations that included *Hall*.

Clearly, *Hall* expressly excludes the "encrypted internal integrity hash" which includes clear form rights information. Applicants also respectfully submit that remaining references do not overcome the previously described deficiency of *Hall* with respect to Claims 1, 2, 4, 9, 11-13, 17, 18, 34, 35, 38, 42, 45, 47, 49, 50, 52, 57, and 59-61 and are therefore believed to be patentable over the cited art. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103(a) to the Claims 1, 2, 4, 9, 11-13, 17, 18, 34, 35, 38, 42, 45, 47, 49, 50, 52, 57, and 59-61 are respectfully requested.

Tampering Detection in Claims 9, 42, and 57

Claims 9, 42, and 57 were rejected under 35 U.S.C. § 103(a) in item 9 on page 7 of the Office Action as being unpatentable over the proposed combination of *Nonaka, Hall, Hardy, Thoma*. With *Nonaka* being the only reference specifically cited against the limitations introduced by Claims 9, 42, and 57. Before discussing *Nonaka* in more detail, it is believed that a brief review of a representative dependent claim will be helpful. Claim 9 calls for, *inter alia*, the method including:

generating a validation hash from at least the clear form rights information;

decrypting the encrypted internal integrity hash to recover the internal integrity hash; and

comparing the validation hash to the internal integrity hash to detect tampering with the rights information.

Accordingly, Claim 9 is directed to obtaining and comparing a validation hash and an encryption hash to determine whether rights information has been tampered with. Simialr language is found in Claims 42 and 57. The Office Action asserts that the elements of Claims 9, 42, and 57 are taught by *Nonaka*. More specifically, the Office Action erroneously alleges that [0246] of *Nonaka* teaches comparison of a validation hash with an internal integrity hash to detect tampering. When [0246] of *Nonaka* is read in context with surrounding material, the limitations of Claims 9, 42, and 57 are clearly not taught. Starting with [0243] of *Nonaka* the following disclosure is found:

> [0243] The directory structure data represents a relationship among the content files CF and a relationship between the content file CF and the key file KF within the secure container 104.

[0244] For example, if content files CF1 through CF3 and the corresponding key files KF1 through KF3 are stored in the secure container 104, a link between the CF1 through CF3 and a link between the content files CF1 through CF3 and the key files KF1 through KF3 are established, as shown in FIG. 9, by the directory structure data.

[0245] The hyperlink data represents a hierarchical structure of the key file KF and a relationship between the content files CF and the key files KF by considering all the files inside and outside the secure container 104.

[0246] More specifically, address information to be linked and the authentication value (hash value) thereof are stored, as shown in FIG. 10, in the secure container 104 for each content file CF and for each key file KF. **The hash value of one content file CF or one key file KF obtained by a hash function H (x) is then compared with that of another file CF or another key file KF to be linked, thereby verifying the link between the files.**

(Emphasis added)

This disclosure by *Nonaka* is limited to comparing hashes of key files, content files, or a key file and a content file **to verify a link between such files**. This, however, is not a teaching or suggestion of comparing a generated "validation hash" to the recovered "the internal integrity hash" to determine whether the clear form rights information has been tampered with.

Moreover, the cited portions of *Nonaka* above also fails to disclose generating a validation hash and decrypting the encrypted internal integrity hash as recited in Claim 9. Each of the other paragraphs ([0019], [0021], and [0027]) cited in *Nonaka* to allegedly teach the other elements of Claim 9 also fail to remedy the deficiencies in [0246]. More specifically, [0019] of *Nonaka* discloses a tamper-resistant circuit module included in a data processing apparatus for performing rights processing of the content data. The tamper-resistant circuit module of *Nonaka* also includes an encryption processing circuit for decrypting content key data. Moreover, [0027] of *Nonaka* indicates that a hash-value generating circuit may exist within the tamper-resistant circuit module to generate hash values of content data, the content key data, and the UCP data. These hash values may be used by the public-key encryption circuit to "create the signature data" ([0027 of *Nonaka*).

However, there is no comparison of a generated validation hash with a decrypted internal integrity hash to detect tampering as recited in Claims 9, 42, and 57 of the instant application. Claims 9, 42, and 57 and are therefore believed to be patentable over the cited art. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103(a) to the Claims 9, 42, and 57 are respectfully requested.

Re-Generation of Internal Integrity Hash in Claims 13 and 61

Claims13 and 61 were rejected under 35 U.S.C. § 103(a) in item 9 on page 7 of the Office Action as being unpatentable over the proposed combination of *Nonaka, Hall, Hardy, Thoma*. Applicant respectfully traverses.

Claim 13 calls for, *inter alia*, the method including:

tracking usage of the content;

updating the clear form rights information with changes in usage; and

for each update of the clear form rights information:

re-obtaining the internal integrity hash of second data comprising the updated clear form rights information, said clear form external integrity hash, and said externally inaccessible client device key; and

re-encrypting, and re-storing the internal integrity hash on the client device.

Accordingly, Claim 13 relates to re-generating an integrity hash comprising (1) rights information; (2) an encryption key; and (3) a first hash that itself comprises (a) **the same rights information as in the second hash**, and (b) an external key. Similar limitations and language are found in claim 61.

As previously discussed above, the proposed combination of *Nonaka, Hall, Hardy* and *Thoma* whether considered alone or in any combination, fail to teach or suggest generating the internal integrity hash of Claim 1 a first time, and therefore cannot teach or suggest re-generating the same hash as recited in Claim 13 a second time. The portions of *Nonaka, Hall,* and *Hardy* cited in the Office Action, which allegedly teach the elements of Claim 13, fail to remedy this teaching deficiency. Claims 13 and 61 and are therefore believed to be patentable over the cited art. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103(a) to the Claims 13 and 61 are respectfully requested.

Externally Inaccessible Data Path in Claim 15

Claim15 was rejected under 35 U.S.C. § 103(a) in item 9 on page 7 of the Office Action as being unpatentable over the proposed combination of *Nonaka, Hall, Hardy, Thoma*. Applicant respectfully traverses.

In yet another example, the elements of Claim 15 are also not taught or suggested by the proposed combination of *Nonaka, Hall, Hardy* and *Thoma*, when considered either alone or in combination. Claim 15, *inter alia*, reads: "...wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path." In contrast, paragraphs [0036] and [0346] of *Nonaka*, which are erroneously alleged to teach Claim 15, both fail to teach or suggest these elements of Claim 15. Specifically, *Nonaka* fails to teach a "client device" comprising a "code embedded in hardware" having "no externally accessible data path." Rather paragraph [0346] of *Nonaka* teaches "the SAM" being "completely shielded from an external source," but the "SAM" as described in this paragraph is a secure application module that is by definition sent on an externally accessible data path from the content provider to the client device. Moreover, the "SAM" of *Nonaka* does not refer to a client device key or to a code that comprises a client device key as in Claim 15, but may incorporate key security mechanisms to secure its data payload. Paragraph [0036] of *Nonaka* teaches that the data processing apparatus may encrypt content key data with license key data having an effective period. Paragraph [0036] of *Nonaka* concludes with the clarification that the common-key encryption circuit (e.g., requires externally accessible datapath to be common) decrypts "the content key data by using the read license key data. The remaining portions of *Nonaka, Hall, Hardy* and *Thoma* do not remedy this teaching deficiency, either alone or in combination, and therefore Claim 15 is also believed to be in condition for allowance. Accordingly, withdrawal of the rejection under 35 U.S.C. § 103(a) to the Claim 15 is respectfully requested.

Request Specific Clarification of Rejections Relative to Claims 10, 43, and 58

Claims 10, 43, and 58 were rejected under 35 U.S.C. § 103(a) in item 11 on page 31 of the Office Action as being unpatentable over *Nonaka, Hall, Hardy, Thoma* and further in view of *Chase*. As previously mentioned, upon review of the stated reasons for rejection of Claims 10, 43 and 58 it appears that the Office Action may not have been examining the most recent version of the amended claims. Moreover, it is believed that the remaining

claims are distinguishable over the proposed combination. Accordingly, Applicant respectfully traverses.

As previously noted the Office Action on page 31 specifically references Claim 32 and Claim 33, both of which were previously canceled, in the rejection. While the inclusion of these canceled claims may simply be disregarded as moot, Applicant is concerned that the Office Action may not have been examining the most recent version of the amended claims and as a result "all words in a claim" were not by definition considered in judging the patentability of that claim as required under MPEP § 2143.03. When this concern is combined with the fact that supporting any rejection under 35 U.S.C. § 103(a) requires a clear articulation of the reasons why the claimed invention would have been obvious (MPEP § 2143), sufficient grounds exist to request specific clarification **in a non-final Office Action.** Accordingly, Applicants respectfully request further clarification of the rejection of Claims 10, 43, and 58 under 35 U.S.C. § 103(a) **in a non-final Office Action** so as to provide the Applicants fair opportunity to reply to the rejection.

Disabling Content upon Detection of Tampering in Claims 10, 43, and 58

Alternatively, Applicant respectfully requests withdrawal of the rejections under 35 U.S.C. § 103(a) to Claims 10, 43, and 58 in view of the arguments presented below.

Before discussing the proposed combination of *Nonaka, Hall, Hardy, Thoma* with *Chase* in detail, it is believed that a brief review of Claim 10 and Claim 43 and Claim 58 will be helpful. Claims 10 calls for, *inter alia*, disabling the content on the client device if tampering is detected. Similar limitations are found in Claims 43, and 58.

The proposed combination of *Nonaka, Hall, Hardy,* and *Thoma* explicitly fails to teach disabling content if tampering is detected. (page 31 of Office Action). In comparison, *Chase* discloses content revocation by disabling licenses for content issued to a computing device, but fails to teach "disabling the content on the client device if tampering is detected" as recited in claim s 10, 43, and 58 of the instant application. Content revocation of *Chase* is limited to an expected termination of rights, such as an invalid license or the expiration of an issued license based on time or usage. However, this content revocation occurs without consideration of tampering to the underlying license. As such, by tampering with the license terms or license expiration a sophisticated and determined user might present an apparently valid license to the system of *Chase* and avoid content revocation. In contrast, the instant

application can detect tampering and properly disable the content on the client device. In one embodiment, tampering may be detected by maintaining an internal integrity hash that is not vulnerable to the actions of the same sophisticated and determined user mentioned previously, because the internal integrity hash is not used outside of the client device, it cannot be replicated or altered and may therefore help detect tampering.

It is accordingly believed to be clear that the proposed combination of *Nonaka, Hall, Hardy, Thoma* and *Chase* neither show nor suggest "**disabling the content** on the client device **if tampering is detected**" as recited in Claims 10, 43, or 58 of the instant application. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103(a) to the Claims 10, 43, and 58 are respectfully requested.

Conclusion

For at least the reasons above, Applicant respectfully submits that all pending claims are allowable and request that the Examiner permit these claims to proceed to issuance. Although additional arguments are believed to exist for distinguishing the cited documents, the arguments presented are believed sufficient to address the Examiner's rejections. Likewise, failure of the Applicant to respond to a position taken by the Examiner is not an indication of acceptance or acquiescence of the Examiner's position. Instead, it is believed that the Examiner's positions are rendered moot by the foregoing arguments, and it is therefore not believed necessary to respond to every position taken by the Examiner with which Applicant do not agree.

The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to AEON Law's deposit account. The deposit account number is 50-4051.

Respectfully submitted,

AEON LAW

Date: October 15, 2010

by: /Kyle H. Flindt/

Kyle H. Flindt, Reg. No. 42,539
Direct: 206.577.1684
E-mail: kyle@aeonlaw.com

AEON Law
1525 4th Avenue, Suite 800
Seattle, WA 98101
Telephone: 206-217-2200
Customer No.: 61,857